AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) Method for monitoring the usage of a service by a communication device coupled to a ~~tamper resistant module, in particular a~~ smart card, said service being transmitted from a resource able to communicate with said communication device by way of a network, said service comprising a plurality of encrypted data flow, the use of said service comprising successive decryption steps of data flow by a respective first key [[EK]], said first key [[EK]] being encrypted in the data flow and decrypted in the ~~tamper resistant module~~ smart card by way of a second key [[KEK]] stored in said ~~tamper resistant module~~ smart card or derived inside said ~~module~~ smart card, characterized in that said method comprises the following steps:
   a. A counting step, in which a memory location stores a count of occurrences of decryption steps of said first key [[EK]] attached to a same service;
   b. A using step, in which said counter is used to ~~prove the amount of data flow which has been decrypted~~ determine a service fee for use of said service.

2. (Currently Amended) Method according to claim 1, characterized in that the ~~module~~ smart card stores a predetermined fixed number, and in that it comprises a comparison step in which the incrementing counter is compared to the predetermined fixed number for checking if the counter has reached or not the value of the fixed number; if yes, adequate action can be performed.

3. (Currently Amended) Method according to claim 1, characterized in that a command is sent to the ~~tamper resistant module~~ smart card for renewing the second key [[KEK]].

4. (Currently Amended) Method according to claim 1, characterized in that a command is sent to the ~~tamper resistant module~~ smart card for Resetting/Updating the counter.

5. (Currently Amended) Method according to claim 3 [[or 4]], characterized in that said command is encrypted by a third key [[(MK)]] known by the ~~tamper resistant module~~ smart card.

6. (Original) Method according to claim 2, characterized in that the action is the completion of decryption steps.

7. (Original) Method according to claim 1, characterized in that, each first key is sent periodically, and in that the amount of data is converted into time of use limiting the use of a service in time.

8. (Currently Amended) Method according to claim 4 [[or 5]], characterized in that said commands are transmitted to the ~~tamper resistant module~~ smart card by way of the communication device, said communication device including a program for authorizing the transmission of such commands without reading its content.

9. (Currently Amended) ~~Data processing module, in particular a~~ A smartcard, able to receive services from a network, said services comprising a plurality of encrypted data flow, the use of said service comprising successive decryption steps of data flow by a respective first key [[EK]], said first key [[EK]] being encrypted in the data flow and decrypted in said ~~module~~ smart card by way of a second key [[KEK]] stored in said ~~module~~ smart card or derived inside said ~~module~~ smart card, characterized in that ~~module~~ smart card comprises a microcontroller able to perform the following steps:

   a. A counting step, in which a memory location stores a count of occurrences of decryption steps of said first key [[EK]] attached to a same service;
   b. A using step, in which said counter is used to ~~prove the amount of data flow which has been decrypted~~ determine a service fee for use of said service.

10. (Currently Amended) Computer program, stored on a smart card, including program code instructions to execute the counting step of the method defined in claim 1, when said program is executed on the smart card ~~a data processing device as defined in claim 9~~.

11. (New) Method according to claim 4, characterized in that said command is encrypted by a third key known by the smart card.

12. (New) Method according to claim 5, characterized in that said commands are transmitted to the smart card by way of the communication device, said communication device including a program for authorizing the transmission of such commands without reading its content.